CLAIMS:

1. A method of securing a hard drive of a computer, comprising:
detecting a portable, physical key with a receiver/decoder circuit associated with the hard drive;
validating the detected key with the receiver/decoder circuit; and
permitting access to the hard drive or a portion thereof with the receiver/decoder circuit if the detected key is validated.

2. The method of claim 1, wherein the receiver/decoder circuit resides in the computer.

3. The method of claim 1, wherein the detecting step includes detecting the key over a secure wireless link.

4. The method of claim 1, wherein the validating step includes determining whether or not the detected key is associated with the hard drive.

5. The method of claim 4, wherein the receiver/decoder circuit enables the hard drive if the detected key is validated and disables the hard drive if the detected key is not validated in order to provide hard drive level protection.

6. The method of claim 5, wherein digital content stored on the computer is not encrypted with the key.

7. The method of claim 4, wherein digital content read from or written to the hard drive is decrypted or encrypted by the receiver/decoder circuit using the key associated with the hard drive in order to provide sector-level protection.

8. The method of claim 4, wherein the key associated with the hard drive is initially delivered with the hard drive.

9. A system for securing a hard drive of a computer, comprising:

a portable, physical key; and

a receiver/decoder circuit for detecting and validating the key and for permitting access to the hard drive or a portion thereof if the detected key is valid, the receiver/decoder circuit being associated with the hard drive;

10. The system of claim 9, wherein the receiver/decoder circuit resides in the computer.

11. The system of claim 9, wherein the receiver/decoder circuit detects the key over a secure wireless link.

12. The system of claim 9, wherein the receiver/decoder circuit validates the key by determining whether or not the detected key is associated with the hard drive.

13. The system of claim 12, wherein the receiver/decoder circuit enables the hard drive if the detected key is validated and disables the hard drive if the detected key is not validated in order to provide hard drive level protection.

14. The system of claim 13, wherein digital content stored on the computer is not encrypted with the key.

15. The system of claim 12, wherein the receiver/decoder circuit decrypts or encrypts digital content read from or written to the hard drive using the key associated with the hard drive in order to provide sector-level protection.

16. The system of claim 12, wherein the key associated with the hard drive is initially delivered with the hard drive.

17. A method of securing and accessing a computer file, comprising:

encrypting the file with a receiver/decoder circuit using a portable, physical key;

storing the encrypted file on a storage medium;

requesting the file with a playback mechanism;

detecting the key with the receiver/decoder circuit;

validating the detected key with the receiver/decoder circuit; and

if the detected key is validated, decrypting the file with the receiver/decoder circuit using the detected key, whereby the decrypted file can be played back with the playback mechanism.

18. The method of claim 17, wherein the storage medium is a hard drive of a computer, and the receiver/decoder circuit resides in the computer.

19. The method of claim 17, wherein a software driver in the computer's operating system instructs the receiver/decoder circuit to perform the detecting, validating, and decrypting steps.

20. The method of claim 17, wherein the detecting step includes detecting the key over a secure wireless link.

21. The method of claim 17, wherein the validating step includes determining whether or not the detected key is associated with the file.

22. A system for securing a computer file and later accessing the file for playback by a playback mechanism, the system comprising:

a portable, physical key;

a receiver/decoder circuit for using the key to encrypt the file; and

a storage medium for storing the encrypted file;

the receiver/decoder circuit for detecting and validating the key and, if the detected key is validated, using the key to decrypt the encrypted file, whereby the decrypted file can be played back with the playback mechanism.

23. The system of claim 22, wherein the storage medium is a hard drive of a computer, and the receiver/decoder circuit resides in the computer.

24. The system of claim 22, wherein a software driver in the computer's operating system instructs the receiver/decoder circuit to detect and validate the key and to use the key to decrypt the file.

25. The system of claim 22, wherein the receiver/decoder circuit detects the key over a secure wireless link.

26. The system of claim 22, wherein the receiver/decoder circuit validates the key by determining whether or not the detected key is associated with the file.